

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

JAMF SOFTWARE, LLC, a limited liability
company,

Plaintiff,

v.

PRAKASH MAHARAJ, an individual, and
KANDJI, INC., a corporation,

Defendants.

No.:

**MEMORANDUM IN SUPPORT OF MOTION FOR TEMPORARY
RESTRAINING ORDER AND EXPEDITED DISCOVERY**

LARKIN HOFFMAN

8300 Norman Center Drive, Suite 1000

Telephone: (952) 896-1541

Fax: (952) 842-1785

amoran@larkinhoffman.com

Andrew D. Moran

**KILPATRICK TOWNSEND
& STOCKTON LLP**

4208 Six Forks Road, Suite 1400

Raleigh, NC 27609

Telephone: (919) 420-1818

Fax: (919) 710-8226

BErwin@kilpatricktownsend.com

Brodie D. Erwin

Pro Hac Vice Application Pending

**KILPATRICK TOWNSEND
& STOCKTON LLP**

1100 Peachtree Street N.E., Suite 2800

Atlanta, GA 30309

Telephone: (404) 815-6522

Facsimile: (404) 815-6555

Drew.Williamson@kilpatricktownsend.com

Andrew T. Williamson

Pro Hac Vice Application Pending

TABLE OF CONTENTS

INTRODUCTION	1
FACTUAL BACKGROUND	3
A. Jamf’s Trade Secrets	4
B. Jamf’s Indian Expansion.....	7
C. Mr. Maharaj’s Contractual Obligations.....	9
D. Mr. Maharaj Terminates his Jamf Contract to Join Kandji	13
E. Mr. Maharaj’s Misappropriation of Trade Secrets	15
F. Mr. Maharaj’s Post-Jamf Usage of Jamf’s Confidential Information to Solicit Customers on Behalf of Kandji	23
G. Defendants Refuse to Adhere to Mr. Maharaj’s Contractual Obligations or Return Jamf’s Misappropriated Trade Secrets	25
ARGUMENT.....	27
A. Legal Standard	27
B. Jamf Satisfies All of the Requirements for Injunctive Relief.....	29
1. Defendants’ Ongoing Possession and Use of Jamf’s Confidential, Proprietary, and Trade Secret Information and Poses a Serious Threat of Irreparable Harm to Jamf	29
C. Jamf Also Has A Significant Likelihood Of Success On The Merits Of Its Claims Against Defendants	31
1. Jamf is likely to succeed on its claim that Mr. Maharaj breached the Service Agreements and NDA.	31
2. Jamf is likely to prevail on its tortious interference claims against Defendants.	32
D. Jamf has a substantial likelihood of prevailing on its trade secret misappropriation claim under the DTSA against Defendants.	34
E. The Balance of Harms Demonstrates That Jamf will Suffer Much Greater Harm If The Injunction Is Not Granted Than Will Defendants If The Injunction Is Granted	38
F. The Public Interest Weighs Heavily In Favor Of Granting An Injunction Against Defendants	39
G. This Court Should Order Expedited Discovery As It Will Facilitate A More Meaningful Preliminary Injunction Hearing	40
CONCLUSION	42

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>3M Co. v. Individuals, Partnerships, & Unincorporated Associations identified in Schedule “A”</i> , No. 20-CV-2348, 2020 WL 6817650 (D. Minn. Nov. 20, 2020).....	42
<i>ALARIS Grp., Inc. v. Disability Mgmt. Network, Ltd.</i> , No. 12-CV-446, 2012 WL 13029504 (D. Minn. May 30, 2012).....	42
<i>Aries Info. Sys., Inc. v. Pac. Mgmt. Sys. Corp.</i> , 366 N.W.2d 366 (Minn. Ct. App. 1985).....	30
<i>ATS Logistics Services, Inc.</i> , No. 04-CV-3975, 2004 WL 2944108 (D. Minn. Dec. 17, 2004)	40
<i>Benefits Admin. Comm. of Brush Aftermarket N. Am., Inc. Grp. Pension Plan v. Wencl</i> , No. 16-CV-2794, 2016 WL 8809478 (D. Minn. Aug. 22, 2016)	42
<i>BMC Software, Inc. v. Mahoney</i> , No. 15-CV-2583, 2015 WL 3616069 (D. Minn. June 9, 2015).....	41
<i>Boston Scientific Corp. v. Duberg</i> , 754 F. Supp. 2d 1033 (D. Minn. 2010)	29
<i>Brightview Grp., LP v. Teeters</i> , 441 F. Supp. 3d 115 (D. Md. 2020)	37
<i>Cherne Indus., Inc. v. Grounds & Assocs.</i> , 278 N.W.2d 81 (Minn. 1979).....	29
<i>CPI Card Grp., Inc. v. Dwyer</i> , 294 F. Supp. 3d 791 (D. Minn. 2018)	34
<i>Creative Communications Consultants, Inc. v. Gaylord</i> , 403 N.W.2d 654 (Minn. Ct. App. 1987).....	30
<i>Cutera, Inc. v. Lutronic Aesthetics, Inc.</i> , 444 F. Supp. 3d 1198 (E.D. Cal. 2020).....	37

<i>Dataphase Sys., Inc. v. C. L. Sys., Inc.</i> , 640 F.2d 109 (8th Cir. 1981)	25, 26
<i>Deluxe Fin. Servs., LLC v. Shaw</i> , No. 16-CV-3065, 2017 WL 3327570 (D. Minn. Aug. 3, 2017)	35
<i>Equus Computer Sys., Inc. v. N. Computer Sys., Inc.</i> , No. 01-CV-657, 2001 WL 1636487 (D. Minn. May 4, 2001).....	29
<i>Freedom Medical, Inc. v. Sewpersaud</i> , 469 F. Supp. 3d 1269 (M.D. Fla. 2020)	37
<i>Guidant Sales Corp. v. Baer</i> , No. 09-CV-0358, 2009 WL 490052 (D. Minn. Feb. 26, 2009)	29
<i>Guidant Sales Corp. v. Niebur</i> , 2001 WL 1636502 (D. Minn. Oct. 18, 2001)	29
<i>Hubbard Feeds, Inc. v. Animal Feed Supplement, Inc.</i> , 182 F.3d 598 (8th Cir. 1999)	25
<i>Hypro LLC v. Reser</i> , No. 04-CV-4921, 2004 WL 2905321 (D. Minn. Dec. 10, 2004)	28
<i>International Ass’n of Machinists v. Northwest Airlines, Inc.</i> , 674 F. Supp. 1387 (D. Minn. 1987)	25
<i>Intertek Testing Servs., N.A., Inc. v. Pennisi</i> , 443 F. Supp. 3d 303 (E.D.N.Y. 2020)	37
<i>Kallok v. Medtronic, Inc.</i> , 573 N.W.2d 356 (Minn. 1998).....	33, 34
<i>Klass v. Twin City Fed. Sav. and Loan Ass’n</i> , 190 N.W.2d 493 (Minn. 1971).....	39
<i>Life Time Fitness, Inc. v. DeCelles</i> , 854 F. Supp. 2d 690 (D. Minn. 2012)	30
<i>loanDepot.com, LLC v. Schneider</i> , ___ F. Supp. 3d ___, 2022 WL 17818550 (N.D. Ill. 2022)	37
<i>Marco Tech., LLC v. Midkiff</i> , No. 19-CV-2323, 2020 WL 12442072	32

<i>Medtronic, Inc. v. Sun</i> , 1997 WL 729168 (Minn. Ct. App. Nov. 25, 1997)	29
<i>Midwest Sign & Screen Printing Supply Co. v. Dalpe</i> , 386 F. Supp. 3d 1037 (D. Minn. 2019).....	42, 43
<i>Modern Controls, Inc. v. Andreadakis</i> , 578 F.2d 1264 (8th Cir. 1978)	29
<i>Moua v. Moua</i> , No. A11-CV-1647, 2012 WL 1970119 (Minn. Ct. App. June 4, 2012).....	38
<i>Nw. Airlines v. Am. Airlines</i> , 853 F. Supp. 1110 (D. Minn. 1994)	35
<i>PepsiCo, Inc. v. Redmond</i> , 54 F.3d 1262 (7th Cir. 1995)	29
<i>Schumacher v. Schumacher</i> , 627 N.W.2d 725 (Minn. Ct. App. 2001).....	39
<i>United Industries Corp. v. Clorox Co.</i> , 140 F.3d 1175 (8th Cir. 1998)	25
<i>Variable Annuity Life Ins. Co. v. Coreth</i> , 535 F. Supp. 3d 488 (E.D. Va. 2021)	37
<i>Vascular Solutions, Inc. v. Pedregon</i> , No. 09-CV-2089, 2009 WL 2743022 (D. Minn. Aug. 26, 2009)	31
<i>Wells Fargo Investments, LLC v. Bengtson</i> , No. 07-CV-3192, 2007 WL 2007997 (D. Minn. July 9, 2007)	26, 28

Statutes

18 U.S.C. § 1832	41
18 U.S.C. § 1835	41
18 U.S.C. § 1836(b)(1)	34
18 U.S.C. § 1839(3).....	34
18 U.S.C. § 1839(5).....	36
18 U.S.C. § 1839(6).....	36

Other Authorities

Federal Rules of Civil Procedure Rule 26(b)	42
Federal Rules of Civil Procedure Rule 65(b)	25

Plaintiff Jamf Software, LLC (“Jamf” or “Plaintiff”) brings this motion seeking a temporary restraining order and expedited discovery to prevent its former Regional Sales Manager, Defendant Prakash Maharaj (“Mr. Maharaj”), from violating the express terms of his confidentiality and non-solicitation obligations with Jamf, and to prevent Mr. Maharaj’s new employer—and Jamf’s direct competitor—Kandji, Inc. (“Kandji”), from continuing to aid and abet Mr. Maharaj’s misappropriation of Jamf’s trade secrets and use of Jamf’s information to solicit its customers on Kandji’s behalf.

INTRODUCTION

Mr. Maharaj *unlawfully exported 350,000 files* containing Jamf’s most sensitive business information just prior to joining Jamf’s direct competitor Kandji. Jamf has now learned that Mr. Maharaj is utilizing these misappropriated trade secrets to unlawfully solicit and steal Jamf customers on Kandji’s behalf in violation of valid agreements he has with Jamf.

Mr. Maharaj was Jamf’s first salesperson in India and responsible for developing, deploying, and supervising Jamf’s strategy for growing and ultimately servicing clients and other business partners in emerging markets, specifically the Indian market. As such, Mr. Maharaj was personally involved in negotiating, or overseeing negotiation of, Jamf’s business relationships with businesses and government entities in India and had direct access to and knowledge of Jamf’s confidential information, including its current and planned strategies for affiliating and maintaining relationships with customers, resellers, and other business partners in India and other emerging markets, such as the Middle East and Africa.

Mr. Maharaj abruptly declined Jamf's offer of employment in early July 2023. Unbeknownst to Jamf at the time, he did so because he had (over the course of many months) negotiated and accepted a new position with Kandji. Unlike Jamf, Kandji has not spent the past five years establishing a presence in the Indian market. In fact, Mr. Maharaj is Kandji's first sales representative in India.

Jamf has now learned that in the days before Mr. Maharaj left Jamf to accept a Director of Sales, India, position with Kandji (which was substantially the same position he held at Jamf), he accessed, and unlawfully exported, a staggering number of Jamf's confidential and proprietary files, including Jamf's highly sensitive sales and customer information. While still under contract with Jamf, Mr. Maharaj surreptitiously created a folder on his company-issued laptop device titled "Transitioning [sic] Out of Jamf" and began exporting *hundreds of thousands of files* from the folder, and other places on his Jamf device, to a personal USB drive. Now, Mr. Maharaj has begun selling the same services and products on behalf of Kandji to the same customers with whom he worked while under contract with Jamf. As explained herein, he is soliciting Jamf's clients by utilizing the Jamf trade secrets he misappropriated, and he is doing this with Kandji's apparent approval and encouragement. Defendants' conduct is in clear violation of valid confidentiality obligations to Jamf and applicable state and federal law.

Remarkably, Defendants have refused to commit to returning or destroying the misappropriated information despite being presented with cease-and-desist letters from Jamf asking them to do so. Thus, Kandji is permitting Mr. Maharaj to retain Jamf's trade secret information and utilize it on Kandji's behalf to solicit and otherwise unlawful

interfere with Jamf’s current and prospective customers. In fact, Jamf is aware of at least four of its customers (existing and prospective) who Mr. Maharaj has solicited on behalf of Kandji, and one which Kandji has already stolen using Mr. Maharaj and the purloined information in his possession. It is apparent to Jamf that Mr. Maharaj and Kandji do not intend to return Jamf’s misappropriated trade secret information or cease violating valid contractual obligations owed to Jamf. To Jamf, Kandji’s motive is clear—it wants to continue to utilize Mr. Maharaj and Jamf’s trade secret information to achieve an unearned jump start on its Indian operations. This is not fair or lawful competition and Defendants should be enjoined.

FACTUAL BACKGROUND

Jamf was founded in 2002 by a former Apple systems administrator. (Comp., ¶ 16; Declaration of Elizabeth Benz, ¶ 4).¹ It is based in Minneapolis, Minnesota, and develops, markets, and sells products and services designed to provide IT administrators the necessary resources to manage Apple products. (Benz Decl., ¶¶ 4-5). Specifically, among other products, Jamf produces Jamf Pro, a mobile device management (MDM) software that enables IT departments to secure, control, monitor, and manage end-user Apple devices. (*Id.* at ¶ 5). Additionally, Jamf offers a suite of security products designed to enable businesses to protect and secure both Mac and iOS devices from cyber threats. (*Id.*).

¹ Hereinafter, citations to the Complaint will be denoted “Comp., ¶ __.” Citations to the exhibits attached to the Complaint will be denoted “Ex. __.” Citations to supporting declarations will be cited as “Decl., ¶ __.”

A. Jamf's Trade Secrets

The software market for supporting and securing Apple devices is highly competitive. (*Id.* at ¶¶ 7, 17). Though Jamf has been entrenched in the market for more than two decades, new competitors arise frequently. (Comp., ¶ 28). A fundamental and important part of Jamf's business therefore involves the creation, development, and maintenance of confidential and proprietary information regarding both Jamf's business – *i.e.*, its operations, the specialized services it provides to its customers, its software – and its customers. (Benz Decl., ¶ 7). Jamf's ability to identify the needs and preferences of existing and prospective clients, and to deliver products and services catering to those needs and preferences, is critical to maintaining its business and growing it globally. (*Id.*). As a result, it has invested a substantial amount of money, time, and energy in identifying and evaluating clients and prospects, as well as developing and customizing products and services for those clients and prospects. (*Id.*).

Jamf employs a large, well-trained sales team to seek and secure new business and to provide service and support to existing clients. (*Id.* at ¶ 8). In the course of dealings with clients and prospective clients, Jamf obtains valuable information, including how its clients and prospective clients operate, the identity and contact information for key client personnel, contract expiration and renewal dates, terms for contracts and proposals, price points for contract renewals, and product and service needs and preferences. (*Id.*). Jamf uses this information to develop, analyze, and compile various internal strategies and information, including, but not limited to, Jamf's marketing and business strategies, business leads and opportunities, sales and related financial data, proprietary pricing

information, product specifications and functionality, work-around issues with Jamf's products and services, test case documents, and employee and contractor contact information. (*Id.* at ¶ 9).

Jamf's client and prospective client information is maintained by Jamf on secure databases, including on Salesforce. (*Id.* at ¶ 10; Declaration of Dino Minutolo, ¶ 6). The confidential information on these secure databases is stored on servers located within the United States. (Minutolo Decl., ¶ 7).

Among the highly confidential and proprietary trade secrets on Jamf's secure databases is specific information regarding Jamf's "go to market" strategy for new and/or emerging markets such as India, the Middle East, and Africa, which includes unique pricing structures, different negotiated deals, and creative solutions for how to attract new business and compete with potential competitors in those markets; information regarding the identity and contact information for prospective and existing clients; detailed terms for contracts and proposals; contract expiration and renewal dates; sales quotes; pricing and discounting information; price points for contract renewals; client-specific needs and preferences, including work-around issues; marketing and business strategies; business leads and opportunities; sales and related financial data; cost of goods information; product specifications and functionality, including specific issues and concerns with product functionalities and services, as well as related workaround and troubleshooting information; and supplier and consultant contact information. (*Id.* at ¶ 8).

The databases also contain an opportunities section detailing what specific clients are looking to purchase, product lists, sales leads (new, current, and prospective

customers), sales stage histories, special pricing requests regarding Jamf's offerings, including instances where Jamf gave a client a discount or rebate. The proprietary information contained on these secure databases related to pricing, customers, and business strategy are considered the "crown jewels" of Jamf's sales team worldwide. (*Id.* at ¶ 8(j); Benz Decl., ¶ 12).

Jamf takes substantial precautions to safeguard the confidential and proprietary trade secret information contained in the secure databases. (Minutolo Decl., ¶ 9). The databases are user authenticated and IP address protected through Okta's single sign-on. Okta's single sign-on is an authentication method that enables users to securely authenticate with multiple applications and websites by using just one set of credentials. Okta's single sign-on allows Jamf to have one set of password security standards across multiple different applications. (*Id.* at ¶ 10). This means that Jamf can set a high, consistent standard for password security because Jamf uses Okta to monitor and enforce those standards across all applications managed by Jamf. (*Id.*).

The secure databases are also accessible only by certain individuals, from certain electronic devices, and only from certain locations or IP addresses. (*Id.* at ¶ 11). Database authentication must also be changed every 90 days and users may not re-use their four most recent passwords. (*Id.*). If a user attempts to reset their password, they must first respond to a security question they previously set up. (*Id.*). If a user attempts to login from an unrecognized IP address, a notification is automatically sent to another device previously authorized by the user before the device is permitted access to Jamf's secure databases. (*Id.*). A security token is required for accessing Jamf's secure databases via a

third-party application for integration, such as Microsoft Excel or Outlook. (*Id.* at ¶ 12). Access to the secure databases is limited to only those individuals who have a legitimate need for the information to effectively carry out their specific job duties. (*Id.* at ¶ 13).

Further, Jamf requires any individual to execute a confidentiality agreement before granting them access to Jamf's secure databases. (*Id.* at ¶ 14). For example, contractors such as Mr. Maharaj are required to execute a Service Agreement containing confidentiality provisions prior to being given authorization to access the secure databases. (*Id.* at ¶ 14, Ex. A). Jamf also requires contractors to execute separate Non-Disclosure and Intellectual Property Assignment Agreements ("NDA") containing confidentiality provisions. (Ex. C). All contractors are also required to attend and complete annual training titled "Protecting Our Data." Mr. Maharaj received this annual training on five separate occasions. (Minutolo Decl., ¶ 15).

Jamf's trade secrets are not readily ascertainable by other persons who could, if aware of this information, obtain economic value from their disclosure or use. (Benz. Decl., ¶ 58). If a competitor was privy to this material, it would be at a significant advantage in the highly competitive MDM and security software market. (*Id.*).

B. Jamf's Indian Expansion

Though a Minnesota-based company, Jamf develops and markets its products and services globally through an international sales force. The international sales force uses Jamf's Trade Secrets to market Jamf's products and services globally to businesses, including educational organizations, and government entities, and also to resellers. Those efforts have resulted in Jamf becoming the leading provider of Apple MDM software

services for businesses and governments worldwide. Indeed, as of 2023, Jamf has approximately 73,500 customers and over 31.3 million Apple devices under management. (Benz. Decl., ¶ 6).

In addition to the superiority of its products and services, Jamf’s global reach has expanded in large part due to its investments in key emerging markets. Most recently, this included India, the Middle East, and Africa. (*Id.* at ¶ 14). Specifically, Jamf identified India as being ideally suited for significant investment due to its status as a hub for technology business and development, client demand, large population, and Apple’s success in the territory. (*Id.* at ¶¶ 14-15).²

Jamf commenced its efforts to grow the Indian market in 2018. (*Id.* at ¶ 16). For the past five years, it has committed considerable financial and time resources on developing relationships in India with resellers, end consumers, commercial enterprises, educational companies, and government entities in India. (*Id.*).

Jamf’s efforts to expand its business in India have been successful. Its revenues in the country have grown ten-fold since 2019. (*Id.* at ¶ 19). Based on the successes of its five-year ramp up efforts in India, Jamf officially launched Jamf India Private Limited (“Jamf India”) – its Indian entity – on August 1, 2023. (*Id.* at ¶ 20).

² Jamf’s foresight appears to have been well-warranted. Apple has recently committed significant investments in manufacturing its products in India and, as of this past month, analysts at Morgan Stanley predict that India will account for 20% of Apple’s user growth over the next five years. See Rohan Goswami, India will account for 20% of Apple’s user growth over the next five years, Morgan Stanley estimates, CNBC, July 17, 2023, <https://www.cnbc.com/2023/07/17/india-will-account-for-20percent-of-apples-user-growth-over-the-next-five-years-morgan-stanley-.html>.

C. Mr. Maharaj's Contractual Obligations

As part of its significant investment in developing the Indian market, Jamf hired a team of twenty sales contractors between 2018 and 2019. (*Id.* at ¶ 16). The team began marketing and selling Jamf's products and services in the country. The first such salesperson was Mr. Maharaj, whom Jamf retained in October 2018. (*Id.* at ¶ 21). Jean-Francois Lesseliers, Jamf's Director, Regional Sales, supervised Mr. Maharaj and the remainder of the Indian sales staff from Jamf's offices in Amsterdam, the Netherlands. (Comp., ¶ 44).

As one of the leaders of Jamf's efforts to foster relationships with customers in India and because of the level of technical knowledge necessary to do so, Mr. Maharaj was given access to Jamf's trade secrets, including Salesforce and other databases. (*Id.* at ¶ 46; Benz Decl., ¶ 24). To protect its legitimate business interests with respect to Jamf's Trade Secrets and confidential information, and its legitimate interest in preserving customer goodwill, Jamf and Mr. Maharaj entered into confidentiality covenants as a condition of his retention. (*Id.* at ¶ 25, Ex. A at ¶ 9).

The first set of confidentiality covenants Mr. Maharaj signed were part of the Service Agreement. Specifically, on October 19, 2018, and later on June 4, 2020, as part of his relationship with Jamf, Mr. Maharaj entered into a Service Agreement (individually, "2018 Service Agreement" and "2020 Service Agreement," and

collectively, “Service Agreement”). (Ex. A). The Service Agreement was later amended again in February 2021. (Ex. C).³

Under the Service Agreement, and in exchange for his continued relationship with Jamf, increased monetary compensation, and other benefits, Mr. Maharaj was given access to Jamf’s confidential and trade secret information, stored on secure databases such as Salesforce. Mr. Maharaj agreed that these trade secrets, confidential information, and other proprietary information, which he would be (and was) given access to, included, but was not limited to, the following information:

- (i) Any and all software programs, derivative works, products and other results of the Services performed by [you] under this Agreement...
- (ii) Any and all technical information of the Company or its customers, including, without limitation, product data and specifications, requirements, methodologies, tools, know-how, formulae, the source code, and other software information, processes, inventions, research projects, and product development;
- (iii) Any and all business information of or relating to the Company or its customers that is not known to the general public, including, without limitation, accounting and financial information, sales and marketing information, research, investment analyses, investment strategies and techniques, investment transactions and holdings, clients...and information concerning “know-how” and information, data and material used or licensed by the Company or its customers, including, but not limited to computer software, programming, research, financial information and analyses, and the like documentation relating thereto;
- (iv) Any and all employee information of the Company;

³ There 2021 amendment did not change any of the contractual provisions material to this dispute.

- (v) Confidential information disclosed to the Company by any third party, including its customers to which [you] ha[ve] access to; and
- (vi) Any personally identifiable information relating to the Company and its customers as made available during the performance of Services hereunder.⁴

(Ex. A at ¶ 9.1(i)-(vi)).

Mr. Maharaj acknowledged and agreed that the aforementioned confidential information “constitutes valuable trade secrets of the Company or its customers, as the case may be.” (*Id.* at ¶ 9.1). He further agreed not to disclose any of this information to any third party and also not to use any of it “for any purpose other than for the performance of Services for [Jamf].” (*Id.* at ¶ 9.2). Mr. Maharaj also agreed to return all such information to Jamf promptly upon termination of the Agreement and acknowledged his confidentiality obligations would survive termination of the Agreement. (*Id.* at ¶¶ 8.2.4, 9.2, 9.5). He agreed that in the event of a breach or threatened breach of the Service Agreement, Jamf would “suffer irreparable harm and will be entitled to injunctive relief to enforce this Agreement.” (*Id.* at ¶ 16.6).

Additionally, Mr. Maharaj agreed that the Service Agreement would be governed by Minnesota law and also to submit any dispute or controversy arising thereunder to “the exclusive jurisdiction of the federal or state courts located in the State of Minnesota...and waive[d] any objection (on the grounds of lack of jurisdiction, forum non-conveniens or otherwise) to the exercise of such jurisdiction over it by any such courts.” (*Id.* at ¶¶ 14.1, 14.5).

⁴ The 2018 and 2020 Service Agreements contain identical confidentiality obligations.

Mr. Maharaj reaffirmed those commitments when executing the NDA on February 4, 2022. (Ex. C). Like the Service Agreement, the NDA contains prohibitions against Mr. Maharaj's unauthorized retention and use of Jamf's confidential information both during and after termination of the parties' relationship.

Specifically, the NDA provides that upon termination of the Service Agreement for any reason, Mr. Maharaj shall promptly deliver to the Company:

all computers, zip drives, storage devices, iPhones, iPads....records...documents, letters, reports, data, tables, tables, calculations and all copies of any of the foregoing which are the property of the Company or which relate in any way to the customers, business, practices or techniques of the Company; and

all other property of the Company and Confidential Information which in any of these cases are in [Mr. Maharaj's] possession or under [his] control.

(Ex. C at ¶ 2).

Similar to the Service Agreement, the NDA defines "Confidential Information" as information relating to the "business, products, and affairs of the Company, its affiliates, and its customers, from which [Jamf] derives benefit or economic gain and is not known publically [sic]...unauthorized use or disclosure of which would harm the Company...."

(*Id.* at ¶ 1). The NDA further defines this information as including, but not limited to:

the identity, business, and needs of the Company's customers; the identity of and plans for the development of new customers by the Company; the business and pricing policies and practices of the Company; the financial condition and affairs of the Company; the Company's business development activities and plans for its existing and prospective lines of business, products, and services; the identity of and nature and terms of Company's business relations with customers, vendors, lenders, independent contractors and employees; any data or information that concerns any software development or

coding performed by the Company; marketing and sales strategies of the Company; Company's...computer software and databases, systems, methods, programming materials, processes, new and developing products, services, and promotion campaigning concepts...form documents including quotes, invoices and purchase order.

(*Id.*).

Under the NDA, Mr. Maharaj also agreed that during the term of his association with Jamf, and all times thereafter, he would not use the confidential information on behalf of, nor divulge it to, any third-party except as required or permitted by Jamf. (*Id.*). He agreed to return to Jamf all such information, on any medium whatsoever, when his relationship with Jamf concluded. (*Id.*).

As with the Service Agreement, Mr. Maharaj agreed that to “enforce or prevent violations” of the NDA, Jamf may apply to a court of competent jurisdiction for, among other things, injunctive or other relief...” or require him to “account and pay over to [Jamf] all compensation, profits, monies, or other benefits derived or received by [Mr. Maharaj] as a result of the breach....” (*Id.* at ¶ 5). Finally, he agreed the NDA would be governed by Minnesota law. (*Id.* at ¶ 6).

D. Mr. Maharaj Terminates his Relationship with Jamf to Join Kandji

In January 2023, Mr. Maharaj notified his supervisor, Mr. Lesseliers, that Kandji had contacted him on LinkedIn to discuss becoming its first salesperson in India. Jamf and Kandji are direct, head-to-head competitors. (Benz Decl., ¶ 38).

Kandji was created in 2019 by Adam Pettit and Mark Daughters, who are currently its Chief Executive Officer and Head of Workplace, respectively. (*Id.* at ¶ 45).

Messrs. Pettit and Daughters are well-known to Jamf. Both were originally introduced to Jamf when they were part of Interlaced, LLC a firm founded by Mr. Daughters that was a sales partner of Jamf starting in 2015. (*Id.*). In late 2018, the two founded Kandji. (*Id.*). Initially, Kandji was a bare-bones product focused merely on checking device profiles against known security baselines. (*Id.*). Later, in 2019, Kandji attempted to build a more full-fledged MDM product, thus entering direct competition against Jamf. (*Id.*). Since that time, Kandji appears to have endeavored to grow its business by following Jamf to various emerging markets and trying to mimic Jamf's business moves in those markets. (*Id.*). Unlike Jamf, however, Kandji has not had a presence in India the past five years. In fact, Mr. Maharaj is Kandji's first salesperson in the country. (*Id.* at ¶ 46).

In April 2023, Mr. Maharaj informed Mr. Lesseliers that he was no longer discussing potential employment with Kandji. (*Id.* at ¶ 39). As Jamf would later learn, Mr. Maharaj's assurance was false. Indeed, on or about April 24, 2023, Mr. Lesseliers was contacted by a colleague who works with one of Jamf's largest business partners. (*Id.* at ¶ 40). The colleague forwarded an email he had received from Steve Sutcliffe, a Vice President for Kandji. (*Id.*). In the email, Mr. Sutcliffe mentioned that Kandji was in discussions with Mr. Maharaj concerning his potential to be its first employee in India. (*Id.*).

In late June 2023, Jamf provided Mr. Maharaj – and its other sales contractors in India – with a written offer of employment with Jamf India in the form of a proposed employment agreement. Mr. Maharaj's contract with Jamf was scheduled to conclude on

July 31, 2023, and under the proposal, his employment with Jamf India would commence on August 1, 2023. (*Id.* at ¶ 41).

However, on July 7, 2023, Mr. Maharaj notified Jamf that he was declining Jamf's offer of employment, meaning the parties' relationship would terminate on July 31, 2023. (*Id.* at ¶ 42).

E. Mr. Maharaj's Misappropriation of Trade Secrets

During his final contracted week of work (July 24, 2023, through July 28, 2023) Mr. Maharaj took PTO that he had saved up. (*Id.* at ¶ 48). Jamf later became aware that Mr. Maharaj may be joining Kandji, a direct competitor, after all. As a result, Jamf engaged its Security Operations ("SecOps") group to investigate Mr. Maharaj's activity on his company-issued devices. (Minutolo Decl., ¶ 17). The investigation revealed that in the days and weeks leading up to his separation from Jamf, Mr. Maharaj engaged in an unprecedented level of economic espionage and theft of trade secrets, having downloaded, copied, and retained a substantial amount of confidential and proprietary information related to Jamf's business, including information from its Salesforce and other secure databases authorization.

To conduct the investigation, SecOps utilized the monitoring function within Jamf Protect, one of its software products, to determine whether Mr. Maharaj unlawfully exported Jamf documents and information to a personal storage device and also whether he took screenshots of sensitive information. (*Id.* at ¶ 18). The screenshots taken initially reported via Jamf Protect were among the screenshots seen being transferred to a personal USB device reported in Splunk and further correlated once a backup of the

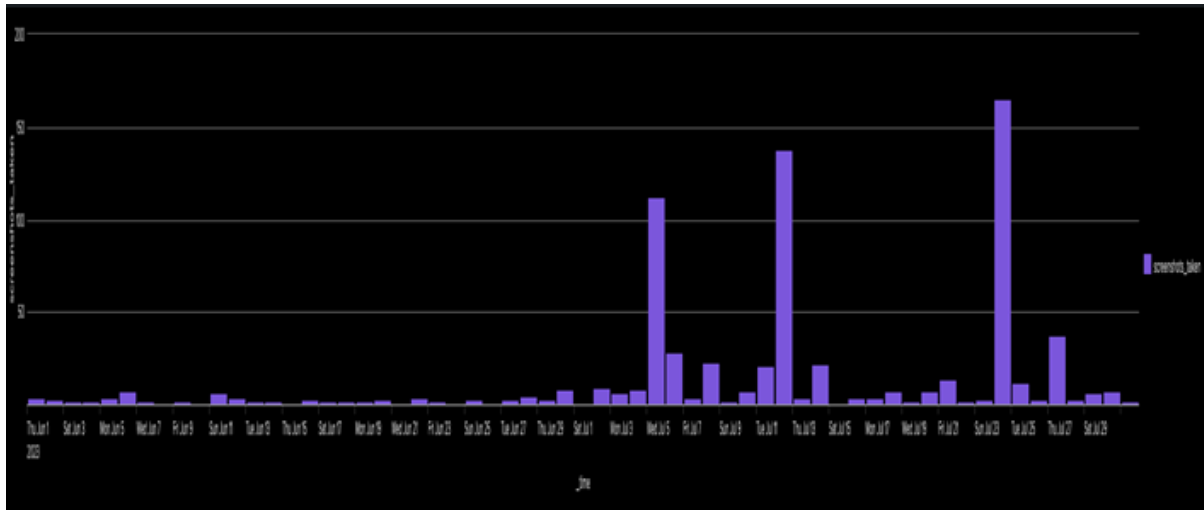
filesystem was provided by IT and investigated by SecOps. (*Id.* at ¶ 19). Splunk is a software tool used by the SecOps team to search, monitor, and analyze machine-generated data via a web-style interface. (*Id.*). Jamf uses Splunk as a security incident event monitoring and investigation tool to centralize event logs across systems. (*Id.*).

This part of the investigation showed that Mr. Maharaj had indeed taken 650 screenshots on his MacBook, including of Jamf's confidential and proprietary information stored on one or more of Jamf's secured databases in the weeks leading up to his departure from Jamf. (*Id.* at ¶ 20, Ex. 1). Hundreds of these screenshots were determined to have been taken within the last few days of his tenure with the Company. (*Id.*). The screenshots taken by Mr. Maharaj included, but are not limited, to:

- a. Jamf's pricing information for customer(s) that Mr. Maharaj worked on for Jamf;
- b. Jamf's report of customer names and value of their bookings for a particular Jamf market that Mr. Maharaj worked on for Jamf;
- c. Jamf's August 2023 quotes for customer(s) showing pricing, volume, and channel discounts; and
- d. Over 150 screenshots of Jamf's presentation for the Jamf 300 course.

(*Id.* at ¶ 21).

The abnormality of Mr. Maharaj's conduct in his final month at Jamf is evident in the spike in screenshot activity reflected in the below chart from InfoSec:



(Minutolo Decl., ¶ 20, Ex. 1). As the chart reflect, InfoSec discovered a significant spike in Mr. Maharaj’s screenshot activity after July 4, 2023.

SecOps’ investigation also looked into USB activity as a potential method for how Mr. Maharaj could have misappropriated Jamf’s confidential and trade secret information in conjunction with his departure from Jamf and new employment with Kandji. (*Id.* at 22). The SecOps team investigated the USB activity by investigating logs from Jamf Protect for screenshots taken on the user's MacBook, Splunk for file copy events, and a loading of the backup received by IT to confirm the contents of files by filename. (*Id.* at ¶ 23).

SecOps discovered that Mr. Maharaj created a folder on his Jamf-issued MacBook titled “Traisitioning [sic] Out of Jamf,” moved Jamf’s confidential and proprietary documents and information to the folder, and ultimately exported the documents and information to a personal USB device that he took with him to Kandji following his last day working for Jamf. (*Id.* at ¶ 24). SecOps determined Mr. Maharaj initially created the “Traisitioning [sic] Out of Jamf” folder on June 30, 2023. (*Id.*). In addition to the files

exported from the “Traisioning [sic] Out of Jamf” folder, Mr. Maharaj also exported files from his desktop to his personal USB device. (*Id.* at ¶ 25). These files also included Jamf’s confidential and proprietary documents, including customer lists and customer-specific presentations. (*Id.*).

The severity and significance of Mr. Maharaj’s actions was only heightened when SecOps discovered the scope of Mr. Maharaj’s USB activity. SecOps’s investigation revealed that in the weeks leading up to his departure from Jamf, Mr. Maharaj downloaded or copied *approximately 350,000 files* to his personal USB device. (*Id.* at ¶ 26).

SecOps filtered the Splunk search to Mr. Maharaj’s local user account. (*Id.* at ¶ 27). In doing so, SecOps was able to confirm that Mr. Maharaj used his system credentials to log into his company-issued MacBook Pro 14 (identified by serial number QG7VFW1GPX) when the USB device was inserted into the MacBook before Mr. Maharaj exported the approximately 350,000 files to the USB device. (*Id.*). Given the immense size of the exported data, SecOps believes Mr. Maharaj copied his entire Jamf drive to his personal USB device. (*Id.* at ¶ 26).

Among the approximately 350,000 files unlawfully downloaded, exported, and retained by Mr. Maharaj are documents related to pricing information for customers, reports regarding customers and their bookings, quotes for customers, and more highly sensitive Jamf business information. (*Id.* at ¶ 27; Benz Decl., ¶¶ 53-54). The majority of the documents and information stolen by Mr. Maharaj, relate to specific clients, sales

divisions, and proprietary pricing information, including, but not limited to the following files:

- a. “Jamf Channel SKU 1002020203”, documents containing targeted information about how Jamf prices and sells various products;
- b. “Jamf Channel SKU 1002020103_001,” same as above;
- c. “Jamf Channel SKU 9001020099-C”, same as above;
- d. “Zoom Info Leads 2023 Q3”, which is a list of Jamf’s sales leads for Q3 or *the current quarter*;
- e. “Q3 India Security Open”, which is a business pipeline list detailing open opportunities to sell Jamf security products for Q3 or *the current quarter*;
- f. “Q3 India All Open Opportunities”, which is a list of all recent sales opportunities that Jamf is tracking in its India sales pipeline for Q3 or *the current quarter*;
- g. “Q3 Marketing Plan Consolidation”;
- h. “India New Logo 2023,” which is a list of Jamf’s new customers;
- i. “Contacts w email 2023”, which is a list of customers;
- j. “EMEIA Partner Contact List”, which is a list of Jamf’s business partners in Europe, the Middle East, India, and Africa;
- k. “India Customer Email Addresses”;
- l. “EMER EDU-Commit & Won” Report, which is a report showing the education customers that Jamf had recently won in its emerging markets; and
- m. Various customer quotes.

(Benz Decl., ¶ 54).

All of the documents and information misappropriated by Mr. Maharaj listed above constitutes confidential and trade secret information under the terms of the Service Agreement and NDA. (*Id.* at ¶ 55; Ex. A at ¶ 9.1; Ex. C at ¶ 1).

Mr. Maharaj's intentional misappropriation of Jamf's proprietary information is further highlighted by the fact that numerous exported files in the "Traisioning [sic] Out of Jamf" folder are titled as "screenshots," "pricing," or specific customer names. (Minutolo Decl., ¶ 28). Leaving no doubt as to his intent to misappropriate the aforementioned confidential and proprietary trade secret information, Jamf's investigation suggests that Mr. Maharaj had actually executed an agreement to join Kandji on July 4, 2023. (Benz Decl., ¶ 52). *Yet, SecOps investigation revealed that the vast majority of Mr. Maharaj's theft took place after that date.* (*Id.*; Minutolo Decl., ¶ 29).

Jamf's investigation also showed that Mr. Maharaj took the Jamf 300 course, a Jamf certification course that provides users a deeper understanding of the macOS and iOS management capabilities within Jamf Pro. (Benz. Decl., ¶ 48; Minutolo Decl., ¶ 30). He took the course in the final days of his relationship with Jamf and weeks after he agreed to join Jamf competitor Kandji. (Benz Decl., ¶ 48; Minutolo Decl., ¶ 30). The Jamf 300 course has a written policy that expressly prohibits recording any part of the training and specifically bans sharing, copying, or reproducing images of training materials in any way. (Benz Decl., ¶ 48; Minutolo Decl., ¶ 31). Despite this express prohibition, Mr. Maharaj took numerous screenshots of the Jamf 300 course programming. (Benz Decl., ¶ 48; Minutolo Decl., ¶ 31). In fact, one of those screenshots is of the presentation page declaring that the course programming is confidential and proprietary to Jamf, and recording is prohibited. (Minutolo Decl., ¶ 30).

Mr. Maharaj has misappropriated all of this confidential information and trade secrets (and more) and is now using it on behalf of, and possibly with, Kandji's direction but certainly its approval, as part of its efforts to unfairly compete against Jamf in India and elsewhere. The misappropriated information is incredibly important to Jamf's business success, its go-forward strategy in India and other emerging markets, and is invaluable to its competitors. (Benz Decl., ¶ 55). This information has been gathered through the significant expenditure of time, resources, and effort, Jamf has spent cultivating customer relationships in India and other emerging markets over the past five years. (*Id.*). The insight Jamf gains from its ongoing dealings with its customers (actual and prospective) is invaluable, as evidenced by the fact that Jamf's customer retention rate is routinely greater than 100%. (*Id.*).

The documents and information Mr. Maharaj misappropriated are also valuable because they contain: the identity and contact information for prospective and existing clients; detailed terms for contracts and proposals; contract expiration and renewal dates; sales quotes; detailed pricing information; price points for contract renewals; client-specific needs and preferences including work-around issues; marketing and business strategies; business leads and opportunities; sales and related financial data; cost of goods information; product specifications and functionality, including specific issues and concerns with product functionalities and services, as well as related workaround and troubleshooting information; and supplier and consultant contact information. (*Id.* at ¶ 56).

Further, the misappropriated information is valuable to Jamf because they contain information: about what specific products various clients are in the market to buy; product lists; sales stage history; and sales pipeline information and leads (new, current, or prospective customers); and special pricing requests showing Jamf products and services and instances where a discount may have been given, among other valuable business information. (*Id.* at ¶ 57).

The Jamf confidential and proprietary information described above is not generally known to the public or the industry in which Jamf operates. (*Id.* at ¶ 58). As a result, if a competitor, like Kandji, becomes privy to this unlawfully misappropriated material, it would be at a significant, unearned, advantage in the highly competitive MDM and security software market. In the hands of a competitor, like Kandji, the customer and pricing information alone would be devastating to Jamf's operations in India and other emerging markets. (*Id.* at ¶ 59). It would allow a competitor to easily identify customers in the market for the types of services provided by Jamf and Kandji and allow Kandji to outbid Jamf by knowing the exact pricing Jamf is charging customers and the products the customers already use or are interested in purchasing. (*Id.*).

On August 3, 2023, Mr. Maharaj e-mailed Mr. Lesseliers and confirmed that he had accepted a position with Kandji as its Sales Director for India, a role that was substantially the same position he had previously held with Jamf. (*Id.* at ¶ 43). However, rather than invest his own talent and Kandji's resources and compete fairly for customers on the merits, Mr. Maharaj decided to raid Jamf by misappropriating its trade secrets and unlawfully soliciting its customers.

F. Mr. Maharaj's Post-Jamf Usage of Jamf's Confidential Information to Solicit Customers on Behalf of Kandji

Immediately after departing from Jamf, Mr. Maharaj began his employment with Kandji. Since joining Kandji, Mr. Maharaj has used the information he unlawfully misappropriated to further Kandji's business interests in violation of his Jamf Agreements as well as applicable state and federal law.

For example, Mr. Maharaj called at least two Jamf customers to solicit their business for Kandji during the week of August 7, 2023. (Benz. Decl., ¶ 62).⁵ The Renewal Customers are currently in renewal negotiations with Jamf. (*Id.*). When departing Jamf for Kandji, Mr. Maharaj was aware of the details of the renewal negotiations, including Jamf's renewal strategy, the renewal terms offered by Jamf, and historical information Jamf had compiled regarding the Renewal Customers. (*Id.*). Importantly, Renewal Customer A and Renewal Customer B were included in a customer list that was downloaded and exported by Mr. Maharaj to his personal USB device, as were documents related to Jamf's strategy for renewal discussions with the customers. (*Id.*).

Mr. Maharaj has also used the unlawfully misappropriated confidential information to solicit prospective customers that Jamf had been actively negotiating with for many months. This includes a customer for whom Mr. Maharaj had recently prepared

⁵ For confidentiality purposes at this stage, Jamf will refer to these customers as "Renewal Customer A," "Renewal Customer B" and, collectively, "Renewal Customers." Jamf is willing to disclose the specific names of the customers once a protective order has been entered.

a price quote on behalf of Jamf. (*Id.* at ¶ 63).⁶ Proprietary information concerning Prospective Customer A's detailed pricing information were included in the documents that Mr. Maharaj unlawfully downloaded and exported. (*Id.*)

Further, Kandji recently won a new account for Prospective Customer B by slightly underbidding Jamf. (*Id.* at ¶ 65).⁷ The information Mr. Maharaj unlawfully misappropriated included numerous documents on Jamf's pricing information for Prospective Customer B, and it is not a coincidence that Kandji submitted a bid and won this account by such a small margin *just days after* Mr. Maharaj joined Kandji as its first salesperson in India. (*Id.*). Thus, it is all but certain that Mr. Maharaj (and Kandji) is using Jamf's misappropriated trade secret information to aid Mr. Maharaj's efforts to solicit these customers on behalf of Kandji.

Though Jamf's investigation remains ongoing, it is aware that Mr. Maharaj misappropriated proprietary information related to at least 20 other customers. (*Id.* at ¶ 66). That number is expected to rise as Jamf continues its forensic investigation. It is likely, if not certain, that Mr. Maharaj has engaged in further customer solicitation in violation of his contractual and legal obligations and will continue to do so absent judicial intervention.

⁶ For confidentiality purposes, this prospective client will be referred to as "Prospective Customer A."

⁷ For confidentiality purposes, this prospective client will be referred to as "Prospective Customer B."

G. Defendants Refuse to Adhere to Mr. Maharaj's Contractual Obligations or Return Jamf's Misappropriated Trade Secrets

On August 8, 2023, Jamf (through its counsel) sent Mr. Maharaj a letter reminding him of his contractual obligations, Jamf's ongoing investigation, and the results of the investigation to date. Jamf requested numerous assurances from Mr. Maharaj, including, but not limited to:

- (a) Written confirmation of his understanding that he is prohibited from using Jamf's confidential information or trade secrets that he obtained while under contract with Jamf;
- (b) Written confirmation of his understanding that he was not allowed to solicit Jamf customers on behalf of himself or Kandji;
- (c) A list and description of any Jamf documents and materials that he had shared with anyone at Kandji or that he had used to further his work for Kandji; and
- (d) Written assurance that he would cooperate with Jamf to immediately return the confidential information and trade secrets.

(Comp., ¶ 98).

Mr. Maharaj responded to Jamf via email on August 10, 2023. In his response, Mr. Maharaj confirmed that he was aware of his post-separation obligations and did not deny that he downloaded, copied, and retained hundreds of thousands of Jamf documents and information in the days leading up to his separation from Jamf. (*Id.* at ¶ 99). However, he refused to confirm that he would return or destroy all Jamf information in his possession.

Jamf (through its counsel) also sent Kandji a letter on August 8, 2023, informing (or reminding it) of Mr. Maharaj's contractual obligations, Jamf's ongoing investigation, and its discovering that Mr. Maharaj had illegally downloaded, copied, exported, and

retained *hundreds of thousands* of files containing Jamf’s confidential and proprietary documents. (*Id.* at ¶ 100). The letter also detailed how Mr. Maharaj was using Jamf’s information to solicit customers for the benefit of Kandji. (*Id.*).

Jamf also requested certain assurances from Kandji, including confirmation as to whether it was aware of Mr. Maharaj’s contractual obligations, confirmation that it would not interfere with those obligations, and confirmation that it had searched its systems and the email of its employees and contractors and confirmed that no Jamf documents or materials were in its possession, and confirmation that it would require Mr. Maharaj to disgorge himself of all Jamf information in his possession. (*Id.* at ¶ 101).

Two days later, Kandji (thorough its internal counsel) responded via email. (*Id.* at ¶ 102). Remarkably, and despite the sheer egregiousness of its employee’s misconduct, Kandji merely confirmed receipt of the letter, that it was reviewing the matter, and would respond “next week” at its leisure. (*Id.*). That same day, Jamf (through its counsel) expressed its dissatisfaction with the non-substantive response. It reminded Kandji that Mr. Maharaj had downloaded and exported more than 350,000 files and was actively using its trade secret information to solicit and steal clients for Kandji. (*Id.*). Jamf further advised Kandji that without a satisfactory and substantive response by Monday, it would be forced to take legal action.

The Monday deadline passed without a response from Kandji. (*Id.* at ¶ 103). To date, neither Mr. Maharaj nor Kandji have returned any of the more than 350,000 files that were misappropriated by Mr. Maharaj. (*Id.*). As a result, Jamf is left with no option but to protect its legitimate business interests through this legal action.

ARGUMENT

A. Legal Standard

A request for a Temporary Restraining Order is governed by Rule 65(b) of the Federal Rules of Civil Procedure, which requires a showing that “immediate and irreparable injury, loss, or damage” will result unless an injunction is issued. Fed. R. Civ. P. 65(b).

In determining whether to grant a temporary restraining order, the Court must consider: (1) the threat of irreparable harm to Jamf; (2) the balance of this harm and any injury that granting the injunction will inflict on Defendants; (3) Jamf’s likelihood of success on the merits; and (4) the public interest (“*Dataphase* factors”). *Dataphase Sys., Inc. v. C. L. Sys., Inc.*, 640 F.2d 109, 113 (8th Cir. 1981); *International Ass’n of Machinists v. Northwest Airlines, Inc.*, 674 F. Supp. 1387, 1391 (D. Minn. 1987). When applying these factors, the Court must “flexibly weigh the case’s particular circumstances” to determine whether the balance of equities favors the moving party such that justice requires the Court to intervene. *Hubbard Feeds, Inc. v. Animal Feed Supplement, Inc.*, 182 F.3d 598, 601 (8th Cir. 1999).

When balancing the equities, no single factor is determinative. *United Industries Corp. v. Clorox Co.*, 140 F.3d 1175, 1179 (8th Cir. 1998). For instance, “where the movant has raised a substantial question and the equities are otherwise strongly in his favor, the showing of success on the merits can be less.” *Dataphase*, 640 F.2d at 113. Thus, the Court must employ a sliding scale in ascertaining whether injunctive relief is appropriate in which the strength of some factors outweigh any weakness in others. *Id.* A

motion for temporary restraining or preliminary injunction motion is “too early a stage of the proceedings to woodenly assess a movant's probability of success on the merits with mathematical precision.” *Wells Fargo Investments, LLC v. Bengtson*, No. 07-CV-3192, 2007 WL 2007997, at *1 (D. Minn. July 9, 2007) (quoting *Gen. Mills, Inc. v. Kellogg Co.*, 824 F.2d 622, 624 (8th Cir. 1987)). Indeed, “where the balance of other factors tips decidedly toward plaintiff, a [] injunction may issue if movant has raised questions so serious and difficult as to call for more deliberate investigation.” *Wells Fargo Investments, LLC*, 2007 WL 2007997, at *1 (D. Minn. July 9, 2007) (quoting *Dataphase*, 640 F.2d at 113). Each of the *Dataphase* factors supports the entry of a temporary restraining order and preliminary injunction here.

In the instant case, Jamf's legal remedy is inadequate and immediate injunctive relief is necessary to prevent irreparable harm. Through Mr. Maharaj's theft, Jamf's direct competitor has access to a plethora of Jamf's confidential and trade secrets information as it relates to the Indian, European, Middle Eastern, and African markets. Kandji has only entered the Indian market this month, with Mr. Maharaj as its first hire, but it has already used some (if not all) of the misappropriated information to undermine Jamf's position in the country.

Indeed, as explained herein, Kandji has already begun using Mr. Maharaj to unlawfully solicit Jamf customers, customers that Mr. Maharaj misappropriated information about in the short period before his separation from Jamf. Jamf must take action now – through expedited discovery – to locate and ultimately have Defendants return all of Jamf's confidential and trade secret information and fully demonstrate they

have done so to prevent further irreparable harm. It also needs the Court to enjoin Defendants from further utilizing Jamf's trade secrets to unlawfully solicit and steal its clients. The damage to Jamf's competitive advantage that results from Defendants' ongoing use and disclosure of Jamf's trade secrets and confidential information, and unlawful solicitation of its clients utilizing the ill-gotten information, can never be fully compensated by an award of damages.

B. Jamf Satisfies All of the Requirements for Injunctive Relief

1. Defendants' Ongoing Possession and Use of Jamf's Confidential, Proprietary, and Trade Secret Information and Poses a Serious Threat of Irreparable Harm to Jamf

The Court should enter immediate injunctive relief for Jamf because it has suffered, and will continue to suffer, irreparable harm if the Court does not do so. Defendants are utilizing misappropriated Jamf trade secrets to unlawfully solicit and steal Jamf's clients. As this Court has stated, "possible damages to [plaintiff's] client relationships and reputation from [plaintiff's] inability to safeguard their confidential information is intangible" and evidence of irreparable harm. *Wells Fargo Investments, LLC*, 2007 WL 2007997, at *2 (D. Minn. July 9, 2007). Courts have also recognized that a company will suffer irreparable harm if employees are not enjoined from using or disclosing the company's confidential information and trade secret information to the company's competitors. *See Hypro LLC v. Reser*, No. 04-CV-4921, 2004 WL 2905321, at *5 (D. Minn. Dec. 10, 2004) (finding that former employer plaintiff would suffer irreparable harm if because the defendants were using the plaintiff's confidential and proprietary information in the marketplace to gain a competitive advantage).

Jamf will suffer irreparable harm to its business and client relationships if it cannot protect its sensitive information in an expeditious manner. Mr. Maharaj (and now Kandji) are in possession of documents containing information related to Jamf's customers, products, pricing, and proprietary business strategies that Mr. Maharaj is now undoubtedly utilizing on behalf of Kandji where he is performing the same job in the same territory that he did for Jamf. (Benz Decl., ¶¶ 55-59). Temporary restraining orders are routinely granted in cases alleging disclosure of confidential information or trade secrets. *See, e.g., Equus Computer Sys., Inc. v. N. Computer Sys., Inc.*, No. 01-CV-657, 2001 WL 1636487, at *3 (D. Minn. May 4, 2001) (granting temporary restraining order: "Given that most of the documents were sent to his home computer after he had apparently decided to work with [a competitor], Defendant Erickson's actions are increasingly suspect"); *see also Modern Controls, Inc. v. Andreadakis*, 578 F.2d 1264, 1270 (8th Cir. 1978) (applying Minnesota law and noting that "[i]t is unrealistic to expect that Andreadakis has not utilized confidential information gained at Modern Controls while working on an identical product at [a competitor]."); *Medtronic, Inc. v. Sun*, 1997 WL 729168, at *4 (Minn. Ct. App. Nov. 25, 1997) (allowing enforcement of noncompete agreement for the purpose of preventing potential or even inadvertent disclosure of confidential information); *Creative Communications Consultants, Inc. v. Gaylord*, 403 N.W.2d 654, 657 (Minn. Ct. App. 1987) (noting district court grant of temporary restraining order against disclosing confidential information and affirming temporary injunction based on threat of disclosure); *Aries Info. Sys., Inc. v. Pac. Mgmt. Sys. Corp.*, 366 N.W.2d 366, 369 (Minn. Ct. App. 1985) (permanent injunctive relief based on

misappropriation of trade secrets proper). As such, the Court should issue the requested injunction in this instance.

C. Jamf Also Has A Significant Likelihood Of Success On The Merits Of Its Claims Against Defendants

Jamf “need only demonstrate that it is likely to succeed on one claim in order to satisfy this prong of *Dataphase*.” See *Life Time Fitness, Inc. v. DeCelles*, 854 F. Supp. 2d 690, 695-96 (D. Minn. 2012) (citing *United Healthcare Ins. Co. v. AdvancePCS*, 316 F.3d 737, 742-43 (8th Cir. 2002)). Nonetheless, Jamf can demonstrate a strong likelihood of success on the merits of *all* its contract, tortious interference, and trade secrets claims against Defendants.

1. Jamf is likely to succeed on its claim that Mr. Maharaj breached the Service Agreement and NDA.

Jamf will be able to show that Mr. Maharaj breached valid contracts with Jamf. Ample evidence available, even at this early stage, demonstrates that Mr. Maharaj breached his Jamf Service Agreement and NDA by retaining and disclosing Jamf’s trade secrets to steal customers on behalf of Kandji and by failing to return the trade secrets at the end of his tenure with Jamf.

A plaintiff has a substantial likelihood of success on the merits of its breach of contract claims when an individual contractually agrees to return all of the plaintiff’s confidential information upon termination of the parties’ relationship but fails to do so. See, e.g., *Vascular Solutions, Inc. v. Pedregon*, No. 09-CV-2089, 2009 WL 2743022, *6 (D. Minn. Aug. 26, 2009) (finding likelihood of success on the merits because defendant “was clearly obligated to return all confidential information in his possession...[but] did

not turn over all confidential and proprietary information to [plaintiff] at the time of his departure from the company.”).

Under both Agreements, Mr. Maharaj had contractual obligations to not retain or disclose Jamf’s confidential and trade secret information and to return any such information in his possession at the time of his separation. (Ex. A at ¶¶ 8.2.4, 9.2, 9.5; Ex. C at ¶¶ 1-2). Instead, he used the final weeks of his relationship with Jamf to export and misappropriate as much of Jamf’s confidential information and trade secrets as possible to aid in his plan to unfairly compete with Jamf on behalf of a direct competitor in the same market. Critically, like the defendant in *Vascular Solutions*, Mr. Maharaj has refused to return any of the information unlawfully misappropriated from Jamf.

2. Jamf is likely to prevail on its tortious interference claims against Defendants.

Jamf is also likely to prevail on both its tortious interference claims against Defendants.

To succeed on a claim for tortious interference with prospective economic advantage, a plaintiff must plausibly allege “(1) the existence of a reasonable expectation of economic advantage belonging to the Plaintiff; (2) the defendant’s knowledge of that expectation; (3) the defendant’s wrongful interference with that expectation; (4) a reasonable probability the plaintiff would have realized the expectation absent the defendant’s conduct; and (5) damages.” *Marco Tech., LLC v. Midkiff*, No. 19-CV-2323, 2020 WL 12442072, at *8 (D. Minn. Feb. 24, 2020) (quoting *Inline Packaging, LLC v. Graphite Packaging Int’l, Inc.*, 164 F. Supp. 3d 1117, 1136 (D. Minn. 2016)).

Here, Jamf has identified several customers whose relationship Defendants have wrongfully interfered with—including at least one prospective customer, Prospective Customer B, that Defendants were able to steal using Jamf’s misappropriated trade secrets. (Benz Decl., ¶¶ 63-65). Jamf will also be able to show that it had a “reasonable expectation” of a continued relationship with its customers, including but not limited to the Renewal Customers, and the economic advantage that accompanies those relationships. Jamf was in the middle of contract renewal discussions with these individuals. (*Id.* at ¶¶ 62-63). As stated in the Benz Decl., Jamf has a customer retention rate that consistently exceeds 100%. (*Id.* at ¶ 55). In the case of Prospective Customer A, Kandji underbid Jamf by \$1,000. (*Id.* at ¶ 65). Jamf believes that Kandji benefited from Mr. Maharaj’s theft of Jamf’s trade secrets to underbid Jamf’s pricing and win the customer. Jamf would have realized the economic advantage with these customers that it was entitled to if not for the unlawful actions of Defendants.

Jamf will also be able to show that Kandji tortiously interfered with its contractual relationship with Mr. Maharaj. To state a claim for tortious interference with contract, a party must allege “(1) the existence of a contract; (2) the accused’s knowledge of the contract; (3) intentional procure of its breach; (4) the absence of justification; (5) damages.” *Kallok v. Medtronic, Inc.*, 573 N.W.2d 356, 362 (Minn. 1998). Further, Minnesota recognizes that interfering with a valid restrictive covenant is an actionable tort. *Id.* In the context of confidentiality, a business’ investment is protected by decreasing that risk that a third party will usurp its “confidential proprietary information.” *Id.* at 361.

As the evidence Jamf has already provided the Court shows, it had valid contracts in the Service Agreement and NDA with Mr. Maharaj that contained confidentiality provisions and required the return of its information upon his separation. (Ex. A at ¶¶ 8.2.4, 9.2, 9.5; Ex. C at ¶¶ 1-2). Jamf sent Kandji a cease-and-desist letter with copies of the contracts and specifically highlighted these sections for them, demanding that they require its employee return Jamf's trade secret information. (Comp., ¶¶ 100-101) However, Kandji has continued to employ Mr. Maharaj without requiring him to return the information he misappropriated. As a result, Jamf has already suffered damages in the loss of at least one prospective customer, and it will likely lose others if an injunction is not entered. Kandji is continuing to encourage and benefit from Mr. Maharaj's contractual violations. It has not and cannot justify its failure to refrain from interfering with Mr. Maharaj's contractual obligations to Jamf in this regard. *See Kallok*, 573 N.W.2d at 362 ("The burden of proving justification is on the defendant.").

3. Jamf has a substantial likelihood of prevailing on its trade secret misappropriation claim under the DTSA against Defendants.

Jamf will also succeed on its federal trade secrets claim against Defendants under the Defend Trade Secrets Act ("DTSA"). The DTSA creates a private cause of action in favor of the owner of a trade secret that is misappropriated "if the trade secret is related to a product or service used in, or intended for use in, interstate or foreign commerce." 18 U.S.C. § 1836(b)(1) (emphasis added). To succeed on a DTSA claim, Jamf must show the existence and misappropriation of a valid trade secret. *CPI Card Grp., Inc. v. Dwyer*,

294 F. Supp. 3d 791, 807 (D. Minn. 2018). The evidence described above demonstrates that Jamf is highly likely to succeed in doing so.

The DTSA defines a “trade secret” as “information” that “(1) is not generally known or readily ascertainable, (2) has value as a result of its secrecy, and (3) is the subject of reasonable efforts under the circumstances to protect its secrecy.” 18 U.S.C. § 1839(3). In its Verified Complaint, Jamf has identified specific information that it contends are its trade secrets, including but not limited to: Jamf’s sales quotes; proprietary pricing information; customer contract expiration and renewal dates; customer renewal strategies, including price points for contract renewals; customer-specific needs and preferences; business leads and opportunities; and product specifications and functionality, including specific issues and concerns with product functionalities and services, as well as related workaround and troubleshooting information. (Comp., ¶ 124).

All of the information enumerated above meets the DTSA definition of a trade secret. The information is not generally known to the public. (Benz Decl., ¶ 58). It has been the subject of reasonable efforts to maintain its secrecy. (Minutolo Decl., ¶¶ 9-15).⁸ The information is used utilized by Jamf to carry out its business and effect sales across state lines and in foreign countries. (Comp., ¶ 126). And the information clearly has competitive and economic value by virtue of its secrecy, as evidenced by, among other

⁸ This Court has held these exact same efforts are reasonable measures to safeguard a company’s trade secret information. *See, e.g., Nw. Airlines v. Am. Airlines*, 853 F. Supp. 1110, 1115 (D. Minn. 1994) (annual policy reminder, restricted access to certain systems, and requiring individuals to execute nondisclosure agreements before accessing materials constitutes reasonable efforts to maintain secrecy).

things, by Defendants’ use of the information to solicit and misappropriate Jamf’s customers. (Benz Decl., ¶¶ 61-65). This Court has routinely held that this exact same type of information should be afforded trade secret protection. *See, e.g., Deluxe Fin. Servs., LLC v. Shaw*, No. 16-CV-3065, 2017 WL 3327570, at *1, 3 (D. Minn. Aug. 3, 2017) (concluding that plaintiff adequately pleaded the existence of trade secrets by alleging that plaintiff misappropriated “customer pricing data, production costs, check unit volumes, profitability, sales analyses, sales strategies, deal structures, sales plans, ‘key account’ data, check program management techniques, and account details (‘Confidential Sales Information’).” (quoting the complaint) (applying DTSA and Ohio's Uniform Trade Secrets Act)).

Jamf will also succeed in proving that Defendants misappropriated its trade secret information. Misappropriation of trade secrets under the DTSA includes the “***acquisition*** of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means[.]” as well as disclosure or ***use*** of a trade secret of another without express or implied consent by a person who used improper means to obtain it, or knew or should have known that improper means were used to obtain it. 18 U.S.C. § 1839(5). “Improper means” includes “theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy[.]” 18 U.S.C. § 1839(6).

The allegations, declarations, and exhibits described above all demonstrate that Mr. Maharaj, and now Kandji through Mr. Maharaj, have ***acquired*** Jamf’s trade secrets without its consent. (Benz Decl., ¶¶ 61-65). The evidence here further demonstrates that Mr. Maharaj ***disclosed*** the trade secrets to Kandji and that Defendants have ***used*** said

trade secrets to unlawfully solicit and steal clients from Jamf. (*Id.*). Trade secret information related to all of the Jamf customers that Mr. Maharaj has contacted on behalf of Kandji can be found in the files he misappropriated. (*Id.*).

Jamf sent demand letters to both Mr. Maharaj and Kandji detailing the improper means through which Mr. Maharaj acquired Jamf's trade secret information. (Comp., ¶¶ 98-101). The letters also disclosed how Mr. Maharaj was using the purloined information to solicit Jamf customers. Defendants simply claim that Mr. Maharaj does not have Jamf's information despite what Jamf's investigation has revealed to be the reality of the situation. Defendants have also made no effort or promise to return the information Mr. Maharaj misappropriated from Jamf. Federal courts routinely grant injunctive relief under similar and far less egregious circumstances. *See, e.g., loanDepot.com, LLC v. Schneider*, __ F. Supp. 3d __, 2022 WL 17818550, at *(N.D. Ill. 2022) (converting temporary restraining order under DTSA into a preliminary injunction where plaintiff demonstrated former employees misappropriated customer data, the former employees did not deny taking the data, and the competitor refused to block the employees' access to the data absent a court order); *Intertek Testing Servs., N.A., Inc. v. Pennisi*, 443 F. Supp. 3d 303, 341 (E.D.N.Y. 2020) (converting temporary restraining order under DTSA into a preliminary injunction where plaintiff submitted evidence that former employee forwarded trade secrets and confidential information to his personal email account, joined a competitor, and solicited plaintiff's customer); *Cutera, Inc. v. Lutronic Aesthetics, Inc.*, 444 F. Supp. 3d 1198, 1206 (E.D. Cal. 2020) (granting temporary restraining order under DTSA where former sales employees transferred trade secret information from company

laptops and were using information for competitor); *Freedom Medical, Inc. v. Sewpersaud*, 469 F. Supp. 3d 1269, 1275 (M.D. Fla. 2020) (converting temporary restraining order under DTSA into a preliminary injunction based on evidence that former employee solicited former employer's clients and prospects and used misappropriated market research in doing so); *Variable Annuity Life Ins. Co. v. Coreth*, 535 F. Supp. 3d 488, 516 (E.D. Va. 2021) (granting injunctive relief against former employees based on evidence that former employees acquired trade secret information and used it to solicit former employers customer); *Brightview Grp., LP v. Teeters*, 441 F. Supp. 3d 115, 132 (D. Md. 2020) (granting injunctive relief based on evidence former employee downloaded trade secrets for personal use). Since Jamf is likely to succeed on the merits of its trade secret claim, the Court should enter an immediate injunction.

D. The Balance of Harms Demonstrates That Jamf will Suffer Much Greater Harm If The Injunction Is Not Granted Than Will Defendants If The Injunction Is Granted

The balance of harms weighs heavily in favor of Jamf and issuance of an injunction. If Jamf does not obtain an injunction its business in India will be decimated as its competitor will be allowed to unlawfully poach its clients using the trade secret information stolen by Mr. Maharaj. It would be difficult, if not impossible, for Jamf to restore its positive relationships with customers and for it to meaningfully retain its goodwill if they are enticed away through unlawful methods. The absence of an injunction will also cause Jamf to lose the benefit of its confidentiality agreements, customer goodwill, and its market position in India and potentially elsewhere. Monetary

damages can never fully compensate Jamf the loss of goodwill, market position, and confidential business information.

On the other hand, an injunction here would simply prohibit Defendants from engaging in improper and unlawful conduct in which they have no right to engage, such as misappropriating Jamf's confidential information. And a temporary restraining order would last only for a short amount of time and would not prohibit Kandji from continuing to employ Mr. Maharaj or doing business India altogether. Rather, it would merely require Defendants to account for and return all of Jamf's confidential information and trade secrets and refrain from soliciting Jamf's customers and prospective customers. *See, e.g., ATS Logistics Services, Inc.*, No. 04-CV-3975, 2004 WL 2944108, at *7 (D. Minn. Dec. 17, 2004) (noting that when a defendant is still able to conduct business and merely "forced to return and to discontinue use of any confidential or trade secret information that was taken from Plaintiff...the balance of harms weighs in favor of the Plaintiff."). The lack of harm to Kandji's business through temporary injunctive relief is further apparent from the fact that until approximately a few weeks ago, it did not have a single employee in India.

E. The Public Interest Weighs Heavily In Favor Of Granting An Injunction Against Defendants

Entering a preliminary injunction is consistent with the public's interest in protecting confidential information and trade secrets. If an immediate injunction is not entered, Defendants will be rewarded for their unscrupulous actions and emboldened to engage in the same unlawful conduct the next time they needed a leg up on their

competition. This does not serve the public interest. *The “public interest demands ‘enforcement of valid business agreements and the protection of legitimate business interests in an industry,’ like the software sector, ‘propelled by vigorous but fair competition.’”* *BMC Software, Inc. v. Mahoney*, No. 15-CV-2583, 2015 WL 3616069, at *10 (D. Minn. June 9, 2015) (quoting *Boston Scientific Corp. v. Duberg*, 754 F. Supp. 2d 1033, 1042 (D. Minn. 2010)). Further, the DTSA expressly authorizes courts to enjoin the misappropriation of trade secrets. *See* 18 U.S.C. § 1835. The existence of criminal penalties for the misappropriation of trade secrets under 18 U.S.C. § 1832 demonstrates just how harmful Congress believes the act of misappropriation is, not just to businesses seeking enforcement, but to society at large. Clearly, enjoining such conduct on the part of Defendants then is in the greater public interest.

Accordingly, consideration of this factor favors issuance of injunctive relief against Defendants.

F. This Court Should Order Expedited Discovery as it Will Facilitate A More Meaningful Preliminary Injunction Hearing

Jamf further respectfully requests expedited discovery pursuant to Rule 26(b) of the Federal Rules of Civil Procedure. Federal Rule of Civil Procedure 26(b) allows expedited discovery where injunctive relief has been sought.

“When considering a motion for expedited discovery, courts apply a ‘good cause’ standard or a standard similar to that of a preliminary injunction.” *3M Co. v. Individuals, Partnerships, & Unincorporated Associations identified in Schedule “A”*, No. 20-CV-2348, 2020 WL 6817650, at *4 (D. Minn. Nov. 20, 2020). “Courts applying the good

cause standard balance the need for the expedited discovery in the administration of justice against the prejudice to the responding party.” *ALARIS Grp., Inc. v. Disability Mgmt. Network, Ltd.*, No. 12-CV-446 (RHK/LIB), 2012 WL 13029504, at *2 (D. Minn. May 30, 2012).

Courts in this Circuit routinely order such expedited discovery upon granting temporary restraining orders. *See Midwest Sign & Screen Printing Supply Co. v. Dalpe*, 386 F. Supp. 3d 1037, 1057 (D. Minn. 2019) (“[C]ourts have found that expedited discovery is appropriate ... when a plaintiff seeks injunctive relief because of the expedited nature of injunctive proceedings.”); *Benefits Admin. Comm. of Brush Aftermarket N. Am., Inc. Grp. Pension Plan v. Wencl*, No. 16-CV-2794, 2016 WL 8809478, at *4 (D. Minn. Aug. 22, 2016) (granting expedited discovery for the “purpose of appropriately tailoring the scope of the TRO and preliminary injunction as necessary to protect Plaintiff’s interests”). Indeed, “[t]he purpose of expedited discovery in the context of a temporary restraining order or preliminary injunction is for ‘[f]urther development of the record before the preliminary injunction hearing,’ which ‘better enable[s] the court to judge the parties’ interests and respective chances for success on the merits.’” *Midwest Sign & Screen Printing Supply Co.*, 386 F. Supp. 3d at 1057–58 (quoting *Edudata Corp. v. Sci. Computs., Inc.*, 599 F. Supp. 1084, 1088 (D. Minn. 1984)).

Here, good cause for expedited discovery exists. Jamf has filed this Motion for Temporary Restraining Order, seeking injunctive relief, concurrent with the filing of its Complaint. Jamf seeks to conduct discovery limited to the issues raised in the instant

Motion for Temporary Restraining Order, including the full extent to which Defendants have misappropriated, are in possession of, and have used Jamf's proprietary trade secrets and confidential information. Expedited discovery in this case will allow for further development of the record and better enable the Court to judge the parties' interests and respective chances for success on the merits.

The discovery sought by Jamf would not impose a significant burden on Defendants. Jamf's requested discovery is related only to documents and information readily available to Defendants. Given the grave nature of Jamf's claims regarding Defendants' misappropriation and misuse of Jamf's confidential information and trade secrets and the pendency of its preliminary injunction motion, expedited discovery is necessary.

Accordingly, Jamf respectfully requests that this Court order the parties engage in expedited discovery over the next thirty days.

CONCLUSION

Immediate injunctive relief is necessary to protect Jamf's confidential information and trade secrets taken by Defendants, particularly given their refusal to return any of the stolen information and blatant use of said information to unfairly compete against Jamf. Accordingly, Jamf respectfully requests that the Court enter an immediate temporary restraining order or preliminary injunction providing the relief Jamf has requested in its Verified Complaint.

Dated: August 17, 2023

/s/ Andrew D. Moran

Andrew D. Moran (0392381)
Larkin Hoffman Daly & Lindgren Ltd.
8300 Norman Center Drive
Suite 1000
Minneapolis, Minnesota 55437-1060
(952) 835-3800
amoran@larkinhoffman.com
Attorneys for Jamf Software, LLC

Brodie D. Erwin
Pro Hac Vice Application Pending
KILPATRICK TOWNSEND & STOCKTON
LLP
4208 Six Forks Road, Suite 1400
Raleigh, NC 27609
Telephone: (919) 420-1818
Fax: (919) 710-8226

Andrew T. Williamson
Pro Hac Vice Application Pending
KILPATRICK TOWNSEND & STOCKTON
LLP
1100 Peachtree Street N.E., Suite 2800
Atlanta, GA 30309
Telephone: (404) 815-6522
Fax: (404) 815-6555

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that:

- (1) This brief complies with D. Minn. LR 7.1;
- (2) This brief (including all text, including headings, footnotes and quotations) contains 10,724 words (lesser than the 12,000 words allowed); and
- (3) This brief has been prepared in a proportionally spaced typeface using Word XP in Times New Roman 13 point font.

This 17th day of August, 2023.

/s/ Andrew D. Moran

Andrew D. Moran (0392381)
Larkin Hoffman Daly & Lindgren Ltd.
8300 Norman Center Drive
Suite 1000
Minneapolis, Minnesota 55437-1060
(952) 835-3800
amoran@larkinhoffman.com
Attorneys for Jamf Software, LLC

Brodie D. Erwin
Pro Hac Vice Application Pending
KILPATRICK TOWNSEND & STOCKTON
LLP
4208 Six Forks Road, Suite 1400
Raleigh, NC 27609
Telephone: (919) 420-1818
Fax: (919) 710-8226

Andrew T. Williamson
Pro Hac Vice Application Pending
KILPATRICK TOWNSEND & STOCKTON
LLP
1100 Peachtree Street N.E., Suite 2800
Atlanta, GA 30309
Telephone: (404) 815-6522
Fax: (404) 815-6555